



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/525,509	03/15/2000	Marcus Peinado	MSFT-0117/147323.1	9495
7590	10/06/2004		EXAMINER	
Steven H Meyer Woodcock Washburn Kurtz Mackiewicz & Norris LLP One Liberty Place 46th floor Philadelphia, PA 19103				HA, LEYNNA A
		ART UNIT	PAPER NUMBER	
		2135		

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/525,509	PEINADO ET AL.
	Examiner	Art Unit
	LEYNNA T. HA	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on _____.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-50 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>4,6</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

1. Claims 1-50 have been examined and is rejected under 35 U.S.C. 103(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over GINTER, Et Al. (US 5,910,987).

As per claim 1:

Ginter, et al. disclose an apparatus for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable and a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request

including an old ((n-1)th) key file having the old sets of black box keys, the apparatus comprising: **[COL. 12, lines 34]**

a code optimizer/randomizer receiving a master executable and randomized optimization parameters as inputs and producing the (n)the executable as an output; **[COL.117, lines 56-62; COL.118, lines 33-35; and COL.204, lines 1-10]**

and a key manager receiving the (n-1)th key file and the (n)th set of black box keys as input **[COL.12, lines 7-15 and COL.118, lines 33-35]**, extracting the old sets of black box keys from the (n-1)th key file **[COL.191, lines 18-66]**, and producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output; **[COL.117, lines 64-67 and 118, lines 35-44]**

wherein the (n)th executable and the (n)th key file are to be forwarded to the requesting DRM system. **[COL.66, lines 46-64]**

[Ginter discloses the memory being updateable and Manager 558 making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). However, Ginter fails to explicitly discuss the process of extracting old keys. It is obvious include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to

retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.]

As per claim 2:

Ginter discusses the apparatus of claim 1 wherein the key manager produces the (n)th key file encrypted according to a secret, the apparatus further comprising an injector receiving the (n)th executable from the code optimizer/randomizer as an input **[COL.118, lines 33-35]**, injecting the secret into the (n)th executable in a pre-determined location, and producing the injected (n)th executable as an output **[COL.118, lines 35-40]**, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system. **[COL.61, lines 23-43 and COL.66, lines 15-64]**

As per claim 3:

Ginter discusses the apparatus of claim 2 wherein the key manager produces the (n)th key file encrypted according to a symmetric key, the apparatus comprising an injector receiving the (n)th executable from the code optimizer /randomizer as an input, injecting the symmetric key into the (n)th executable in a pre-determined location **[COL.65, lines 22-37 and COL.68, lines 50-63]**, and producing the injected (n)th executable as an output, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system. **[COL.61, lines 23-43 and COL.66, lines 15-64]**

As per claim 4:

Ginter discusses the apparatus of claim 2 wherein the (n)th set of black box keys includes a public - private key pair, and wherein the key manager produces the (n)th key file encrypted according to the private key, the apparatus comprising an injector receiving the (n)th executable from the code optimizer/randomizer as an input, injecting the private key into the (n)th executable in a pre-determined location **[COL.65, lines 22-37 and COL.68, lines 50-63]**, and producing the injected (n)th executable as an output, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system. **[COL.61, lines 23-43 and COL.66, lines 15-64]**

As per claim 5:

Ginter discusses the apparatus of claim 2 wherein the injector injects the secret into the (n)th executable in the pre-determined location such that the secret is hidden except to the (n)th executable. **[COL.67, lines 45-57 and COL.68, lines 50-63]**

As per claim 6:

Ginter discusses the apparatus of claim 2 wherein the DRM system resides on a computing device has a hardware ID (HWID) associated therewith, wherein the HWID is included in and obtained from the (n-1)th key file, and wherein the injector injects the obtained HWID into the (n)th executable in a pre-determined location. **[COL.200, lines 58-63 and COL.203, lines 57-65]**

As per claim 7:

Ginter discusses the apparatus of claim 2 wherein the code randomizer produces a help file as an output, the help file specifying how the secret is to be injected into the (n)th executable by the injector, and wherein the injector receives the help file as an input and injects the secret into the (n)th executable according to the help file. **[COL.75, lines 16-27 and COL.117, lines 55-62]**

As per claim 8:

Ginter discusses the apparatus of claim 7 wherein the code randomizer produces the help file as an embedded portion of the (n) executable. **[COL.75, lines 16-27 and COL.117, lines 55-62]**

As per claim 9:

The apparatus of claim 1 further comprising a signature generator receiving the (n)th executable as an input, generating a digital signature for the (n)th executable, coupling the generated digital signature to the (n)th executable, and producing the coupled (n)th executable and digital signature as an output, wherein the coupled (n)th executable and digital signature and the encrypted (n)th key file are to be forwarded to the requesting DRM system.

[COL.137, lines 38-45 and COL.139, lines 13-17]

As per claim 10:

Ginter discloses a method for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM

system upon request therefrom and including a new ((n)th) executable and a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request including an old ((n-1)th) key file having the old sets of black box keys, the method comprising:

[COL.6-COL.14]

receiving a master executable and randomized optimization parameters;

[COL.66, lines 15-32 and COL.117, lines 56-62]

producing the (n)th executable based on the received master executable and the received randomized optimization parameters and based on a code optimization/randomization technique; **[COL.118, lines 33-35 and COL.204, lines 1-10]**

receiving the (n-1)th key file and the (n)th set of black box keys; **[COL.12, lines 7-15]**

extracting the old sets of black box keys from the (n-1)th key file;

[COL.191, lines 18-66]

producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output based on the extracted old sets of black box keys from the (n-1)th key file and the received (n)th set of black box keys; and **[COL.117, lines 64-67 and 118, lines 35-44]**

forwarding the produced (n)th executable and the produced (n)th key file to the requesting DRM system. **[COL.66, lines 46-64]**

[Ginter discloses the memory being updateable and Manager 558 making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65).

However, Ginter fails to explicitly discuss the process of extracting old keys. It is obvious to include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.]

As per claim 11:

The method of claim 10 wherein the old sets of keys in the (n-1)th key file are encrypted according to a secret of an (n-1)th executable, and wherein extracting the old sets of keys comprises obtaining the secret of the (n-1)th executable and applying the secret to the encrypted old sets of keys in the (n-1)th key file. **[COL.191, lines 18-66]**

As per claim 12:

Ginter discusses the method of claim 11 wherein the request includes the (n-1)th executable, wherein the secret is embedded in the (n-1)th executable, and wherein obtaining the secret of the (n-1)th executable comprises extracting the secret from the (n1)th executable. **[COL.191, lines 18-66]**

As per claim 13:

Ginter discusses the method of claim 11 wherein the secret is maintained in a database, and wherein extracting, the old sets of keys comprises obtaining the secret from the database. **[COL.68, lines 50-63 and COL.117, lines 64-67]**

As per claim 14:

Ginter discusses the method of claim 11 wherein the secret is included in the (n-1)th key file, and wherein extracting the old sets of keys comprises obtaining the secret from the (n-1)th key file. **[COL.191, lines 18-66]**

As per claim 15:

The method of claim 14 wherein the secret is included in the (n-1)th key file encrypted according to a super secret (SUPER(secret)), and wherein extracting the old sets of keys comprises obtaining (SUPER(secret)) from the (n-1)th key file, obtaining the super secret, and applying the super secret to (SUPER(secret)) to obtain the secret. **[COL.191, lines 18-66; Ginter fails to explicitly discuss the extracting of the old keys. Ginter obviously include extracting the old keys from the key file by being able to retrieve specific**

keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.

Thus, it is obvious in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified.]

As per claim 16:

Ginter discusses the method of claim 10 wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret. **[COL.118, lines 30-65 and COL.191, lines 18-66]**

As per claim 17:

The method of claim 16 wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret derived from the (n)th set of black box keys. **[COL.118, lines 30-65 and COL.191, lines 18-66]**

As per claim 18:

Ginter discusses the method of claim 16 wherein producing the (n)th executable comprises embedding the secret therein. **[COL.35, line 57 - COL.36, line 36 and COL.192, lines 7-32]**

As per claim 19:

Ginter discusses the method of claim 16 further comprising maintaining the secret in a database. **[COL.68, lines 50-63 and COL.117, lines 64-67]**

As per claim 20:

The method of claim 16 wherein producing the (n)th key file further includes placing the secret in the (n)th key file. **[COL.35, line 57 - COL.36, line 36 and COL.67, lines 45-45]**

As per claim 21:

Ginter discusses the method of claim 20 wherein producing the (n)th key file further includes encrypting the secret according to a super secret (SUPER(secret)) and placing (SUPER(secret)) in the (n)th key file. **[COL.191, lines 18-66; Ginter fails to explicitly discuss the extraction process. However, Ginter obviously include extracting the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys. Thus, it is obvious in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified.]**

As per claim 22:

Ginter discusses the method of claim 10 wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-1)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the (n-1)th key file, and wherein producing the (n)th key file comprises inserting the extracted HWID into the (n)th key file.

[COL.35, line 57 - COL.36, line 36 and COL.203, lines 57-65]

As per claim 23:

Ginter discusses the method of claim 10 wherein producing the (n)th executable comprises producing the (n)th executable with space reserved

therein for additional information. **[COL.75, lines 16-27 and COL.117, lines 55-62]**

As per claim 24:

Ginter discusses the method of claim 23 wherein producing the (n)th executable comprises producing the (n)th executable with space reserved therein for additional information to be injected by an injector. **[COL.35, line 57 - COL.36, line 36 and COL.75, lines 16-27]**

As per claim 25:

Ginter discusses the method of claim 23 wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-I)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the (n-1)th key File, and wherein producing the (n)th executable comprises injecting the extracted HWID into at least a portion of the reserved space. **[COL.35, line 57 - COL.36, line 36 and COL.200, lines 58-63 and COL.203, lines 57-65]**

As per claim 26:

~~Ginter discusses the method of claim 23 wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret, and wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space.~~
[COL.35, line 57 - COL.36, line 36 and COL.203, lines 57-65]

As per claim 27:

Ginter discusses the method of claim 26 wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret, and wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space in a manner hidden except to the (n)th executable. **[COL.35, line 57 - COL.36, line 36; COL.67, lines 44-46 and COL.68, lines 50-63]**

As per claim 28:

Ginter discusses the method of claim 10 wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-l)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the (n-l)th key file, and wherein producing the (n)th executable comprises producing the (n)th executable based at least in part on the extracted HWID and based on a code optimization/randomization technique. **[COL.35, line 57 - COL.36, line 36 and COL.203, lines 57-65]**

As per claim 29:

Ginter discloses the method of claim 10 comprising:

receiving, at a code optimizer/randomizer, a master executable and randomized optimization parameters as inputs; **[COL.66, lines 15-32 and COL.117, lines 56-62 and COL.204, lines 1-10]**

producing; at the code optimizer/randomizer, the (n)th executable as an output based on the inputs thereto; receiving, at a key manager, the (n-1)th key file and the (n)th set of black box keys as inputs; **[COL.12, lines 7-15 and COL.118, lines 33-35]**

extracting, at the key manager, the old sets of black box keys from the (n-1)th key file; producing; **[COL.191, lines 18-66]**

at the key manager, the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output **[COL.117, lines 64-67 and 118, lines 35-44]** based on the inputs thereto; and forwarding the produced (n)th executable and the produced (n)th key file to the requesting DRM system. **[COL.66, lines 46-64]**

As per claim 30:

Ginter discloses the method for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable, the method comprising:

receiving a master executable and randomized optimization parameters; producing, the (n)th executable based on the received master executable and the received randomized optimization parameters and based on a code optimization/randomization technique; and **[COL.204, lines 1-10]**

forwarding the produced (n)th executable to the requesting DRM system.

[COL.66, lines 46-64]

[Ginter discloses the memory being updateable and Manager 558 making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). However, Ginter fails to explicitly discuss the process of extracting old keys. It is obvious to include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.]

As per claim 31:

Ginter discusses the method of claim 30 wherein producing the (n)th executable comprises producing the (n)th executable with space reserved therein for additional information. **[COL.75, lines 16-27 and COL.117, lines 55-62]**

As per claim 32:

Ginter discusses the method of claim 31 wherein producing the (n)th executable comprises producing the (n)th executable with space reserved

therein for additional information to be injected by an injector. **[COL.35, line 57 - COL.36, line 36 and COL.75, lines 16-27]**

As per claim 33:

Ginter discusses the method of claim 31 wherein the DRM system resides on a computing device having a hardware ID (HVVID) associated therewith, wherein the request from the DRM system includes the HWID, and wherein producing the (n)th executable comprises injecting the included HWID into at least a portion of the reserved space. **[COL.35, line 57 - COL.36, line 36 and COL.200, lines 58-63 and COL.203, lines 57-65]**

As per claim 34:

Ginter discusses the method of claim 31 wherein the (n)th black box further includes a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, wherein the (n)th key file is produced to include the (n)th set of black box keys and the old sets of black box keys encrypted according to a secret, and wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space.

[COL.35, line 57 - COL.36, line 36; COL.67, lines 44-46 and COL.68, lines 50-63]

As per claim 35:

Ginter discusses the method of claim 34 wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved

space in a manner hidden except to the (n)th executable. **[COL.67, lines 45-57 and COL.68, lines 50-63]**

As per claim 36:

Ginter discusses the method of claim 30 wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the request from the DRM system includes the HWID, and wherein producing the (n)th executable comprises producing the (n)th executable based at least in part on the included HWID and based on a code optimization randomization technique.

[COL.203, lines 57-65]

As per claim 37:

Ginter discusses the method of claim 30 comprising:
receiving, at a code optimizer/randomizer, a master executable and randomized optimization parameters as inputs; and producing, at the code optimizer/randomizer, the (n)th executable as an output based on the inputs thereto. **[COL.117, lines 64-67 and 118, lines 35-65]**

As per claim 38:

Ginter discusses the method for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) key file, the (n)th

key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request including an old ((n-1)th) key file having the old sets of black box keys, the method comprising:

receiving the (n-1)th key file and the (n)th set of black box keys; **[COL.66, lines 15-32 and COL.117, lines 56-62 and COL.204, lines 1-10]**

extracting the old sets of black box keys from the (n-1)th key file; and
[COL.191, lines 18-66]

producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output based on the extracted old sets of black box keys **[COL.117, lines 64-67 and COL.203, lines 57-65]**; and forwarding the produced (n)th key file to the requesting DRM system **[COL.66, lines 46-64]**.

[Ginter discloses the memory being updateable and Manager 558 making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). However, Ginter fails to explicitly discuss the process of extracting old keys. It is obvious include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for

verification and referencing purposes in order to produce a new set of black box keys.] [COL.117, lines 64-67 and 118, lines 35-44] [COL.204, lines 1-10]

As per claim 39:

Ginter discusses the method of claim 38 wherein the old sets of keys in the (n-1)th key file are encrypted according to a secret of an (n-1)th executable, and wherein extracting the old sets of keys comprises obtaining the secret of the (n-1)th executable and applying the secret to the encrypted old sets of keys in the (n-1)th key file. **[COL.191, lines 18-66]**

As per claim 40:

Ginter discusses the method of claim 39 wherein the (n)th black box further includes a new ((n)th) executable, wherein the request includes the (n-1)th executable, wherein the secret is embedded in the (n-1)th executable, and wherein obtaining the secret of the (n-1)th executable comprises extracting the secret from the (n-1)th executable. **[COL.191, lines 18-66]**

As per claim 41:

Ginter discusses the method of claim 39 wherein the secret is maintained in a database, and wherein extracting the old sets of keys comprises obtaining the secret from the database. **[COL.68, lines 50-63 and COL.117, lines 64-67]**

As per claim 42:

The method of claim 39 wherein the secret is included in the (n-1)th key file, and wherein extracting the old sets of keys comprises obtaining the secret from the (n-1)th key file. **[COL.191, lines 18-66]**

As per claim 43:

Ginter discusses the method of claim 40 wherein the secret is included in the (n-1)th key file encrypted according to a. super secret (SUPER(secret)), and wherein extracting the old sets of keys comprises obtaining (SUPER(secret)) from the (n-1)th key file, obtaining the super secret, and applying the super secret to (SUPER(secret)) to obtain the secret. **[COL.191, lines 18-66]**

As per claim 44:

Ginter discusses the method of claim 38 wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret. **[COL.67, lines 45-47 and COL.191, lines 18-66]**

As per claim 45:

Ginter discusses the method of claim 44 wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret derived from the (n)th set of black box keys. **[COL.67, lines 45-47 and COL.191, lines 18-66]**

As per claim 46:

Ginter discusses the method of claim 44 further comprising maintaining the secret in a database. **[COL.68, lines 50-63 and COL.117, lines 64-67]**

As per claim 47:

Ginter discusses the method of claim 44 wherein producing the (n)th key file further includes placing the secret in the (n)th key file. **[COL.35, line 57 - COL.36, line 36 and COL.67, lines 45-45]**

As per claim 48:

Ginter discusses the method of claim 47 wherein producing the (n)th key file further includes encrypting the secret according to a super secret (SUPER(secret)) and placing (SUPER(secret)) in the (n)th key file. **[COL.67, lines 45-47 and COL.191, lines 18-66]**

As per claim 49:

Ginter discusses the method of claim 38 wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-1)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the (n-1)th key file, and wherein producing the (n)th key file comprises inserting the extracted HWID into the (n)th key file.

[COL.203, lines 57-65 and COL.191, lines 18-66]

~~As per claim 50:~~

Ginter discloses the method of claim 38 comprising:

receiving, at a key manager, the (n-1)th key file and the (n)th set of black box keys as inputs; **[COL.117, lines 64-67 and COL.118, lines 33-35]**

extracting, at the key manager, the old sets of black box keys from the (n-1)th key file; and **[COL.191, lines 18-66; Ginter fails to explicitly]**

discuss the extraction process. However, Ginter obviously include extracting the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys. Thus, it is obvious in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified.]

producing, at the key manager, the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output based on the inputs thereto. [COL.118, lines 35-65]

Conclusion

****For further information and more details on the rejections above, please refer to Ginter, et al. on col.1, line 47 - Et SEQ.**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax

phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*****TC 2100 will be moved to Carlyle in October 2004. At this time, any inquiry or communications should be directed to the examiner, LEYNNA HA, whose new telephone number is (571) 272-3851 and the new telephone number for TC 2100 receptionist is 571-272-2100.**

LHa


KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100